ARMADILHAS E PERIGOS DO MUNDO DIGITAL


Vinícius Perallis
CEO na Perallis Security
Perallis
HACK3R_
RANGERS

Brasileiros estão entre os mais atacados por golpes durante a pandemia

1 a cada 8 brasileiros acessou ao menos um link que direcionava a páginas maliciosas(Abril á Junho/2020)

Fonte: https://www.kaspersky.com.br/blog/brasil-phishing-covid-golpe/15902/

Mais da metade das pessoas **(52%)** tem seus perfis nas mídias sociais definidos como "Público".

https://blog.lastpass.com/2020/06/maintaining-privacy-and-security-when-sharing-on-social-media-html/

40% dos entrevistados no Brasil disseram já tinham recebido, por exemplo, e-mails de phishing com o tema COVID-19

Fonte: https://www.kaspersky.com.br/about/press-releases/2020_67-dos-funcion-rios-no-receberam-orienta-es-de-ciberseguran-a-para-o-trabalho-remoto

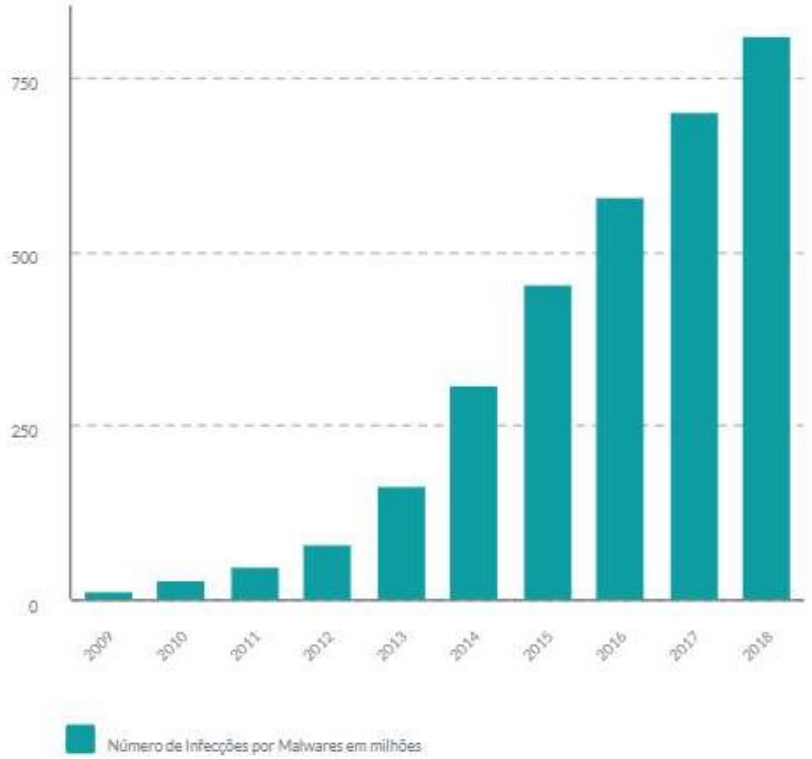
98% dos ciberataque dependem de **engenharia social** para seu sucesso.

Fonte: https://purplesec.us/resources/cyber-security-statistics/

Número de Infecções de Malwares dos últimos 10 anos.

- 2009 - 12.4 milhões
- 2010 - 29.97 milhões
- 2011 - 48.17 milhões
- 2012 - 82.62 milhões
- 2013 - 165.81 milhões
- 2014 - 308.96 milhões
- 2015 - 452.93 milhões
- 2016 - 580.40 milhões
- 2017 - 702.06 milhões
- 2018 - 812.67 milhões

92% dos malwares foram "entregues" por e-mail



Fonte: https://purplesec.us/resources/cyber-security-statistics/

Por que se preocupar com segurança da informação?

"Golpe clona contas de WhatsApp para pedir dinheiro a contatos de vítimas"

Pessoas que anunciam produtos em plataformas como OLX, WebMotors, ZapImóveis e Mercado Livre são alvos de um novo golpe de clonagem de conta no WhatsApp.

“verificamos um anúncio recém postado, e gostaríamos de atualizar para que continue disponível para visualização” ou “devido ao grande número de reclamações referente ao seu número de contato, estamos verificando”

Por que se preocupar com segurança da informação?

Por que se preocupar com segurança da informação?

"Golpe clona contas de WhatsApp para pedir dinheiro a contatos de vítimas"

"Ele mandou mensagens particulares e falou que o limite dele de transferências estava excedido (...) e perguntou qual meu limite de transferências. Falei: 'olha, só posso transferir R$ 800'.

Ele falou 'não tem problema, transfere para essa conta que eu vou te dizer'. E aí foi isso que eu fiz, achando que era o meu pai", relata uma das filhas.

Como ativar a verificação em duas etapas

Passo 1: Abra o WhatsApp e acesse o menu do aplicativo simbolizado pelos três pontinhos no canto superior direito da tela.

Passo 2: Na aba aberta, clique em "Configurações".

Passo 3: Agora, acesse a opção "Conta".

Passo 4: Clique em "Verificação em duas etapas".

Passo 5: Na nova tela, clique em "Ativar" para iniciar a configuração do recurso.

Passo 6: Neste momento, você deverá criar uma senha de seis dígitos (PIN) e confirmar o código escolhido. Depois, também será possível registrar um endereço de e-mail para recuperar o código caso seja necessário.

Passo 7: Depois da personalização, toque em "Concluído" para finalizar a configuração do recurso.

O Pix chegou, mas... Como usá-lo com segurança?

O novo método de pagamentos do Banco Central promete facilitar a vida de todo mundo na hora de transferir valores de forma eletrônica, mas é preciso ficar de olho em golpes

Revolucionário no sistema financeiro global, esse novo método de pagamentos chamou atenção por ser totalmente digital e por possibilitar a transferência de valores 24 horas por dia, sete dias por semana, de forma praticamente instantânea e sem taxas ao consumidor final.

O Pix chegou, mas... Como usá-lo com segurança?

Obviamente, nem tudo são flores. Embora o Pix tenha sido desenhado ao lado de especialistas em segurança cibernética para que ele seja o mais confiável possível, sua estreia acabou criando uma série de ameaças digitais que todo internauta precisa levar em consideração ao usufruir de seus benefícios. Os primeiros riscos, naturalmente, são as campanhas de phishing.

O Pix chegou, mas... Como usá-lo com segurança?

A clássica pescaria

Para usar o Pix, o correntista precisa fazer um cadastro adicional para registrar suas chaves — a "informação" que o pagador precisa para te identificar no sistema e realizar a transferência. Nas semanas em que a plataforma foi lançada, especialistas alertaram para uma grande onda de e-mails falsos tentando roubar informações sensíveis de internautas usando a novidade como isca.

O Pix chegou, mas... Como usá-lo com segurança?

Olha a privacidade!

O Pix permite que você cadastre diversas informações como chaves de identificação, como: CPF, Telefone ou e-mail do correntista. Embora possa parecer muito prático, você tem outra alternativa à sua disposição: chaves temporárias, que são códigos alfanuméricos que podem ser criados e excluídos à vontade.

O Pix chegou, mas... Como usá-lo com segurança?

De olho nas fraudes

Porém, se o cadastramento de chaves aleatórias é um benefício para proteger a sua privacidade, ele também pode virar uma arma nas mãos dos criminosos. Da mesma forma que, hoje em dia, você já pode receber um boleto falso por e-mail, também vai se tornar comum vermos golpistas personificando grandes marcas e usando chaves aleatórias para receber pagamentos de internautas desatentos.

Fique de olho! Ao informar a chave Pix, o próprio sistema retorna algumas informações do beneficiário da transferência, incluindo nome completo.

Descubra se seus dados já foram comprometidos

No site abaixo, basta você colocar seu e-mail e descobrir se você já teve seus dados comprometidos em sites web.

https://haveibeenpwned.com/

Como empresas são afetadas?

Ações da Equifax despencam após roubo de dados de americanos

Como empresas são afetadas?

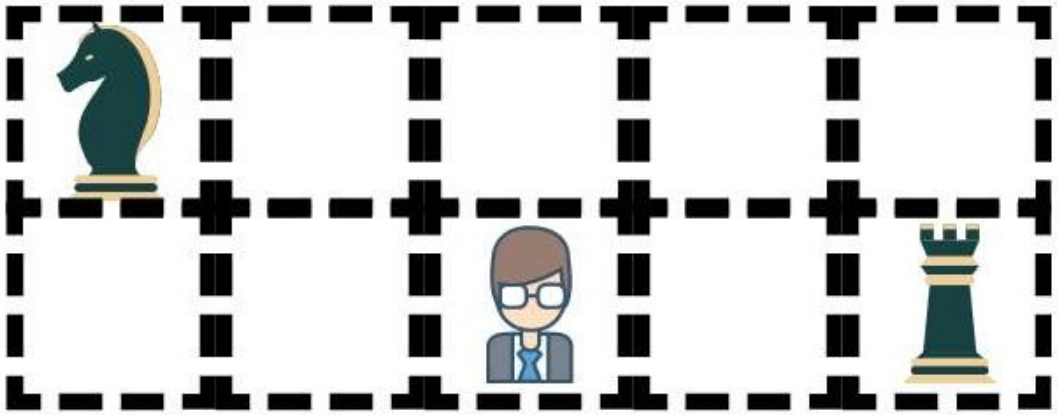
Equifax pagará US$ 575 milhões aos EUA por ciberataque de 2017

https://noticias.uol.com.br/ultimas-noticias/efe/2019/07/22/equifax-pagara-us-575-milhoes-aos-eua-por-ciberataque-de-2017.htm

Táticas de Engenharia Social

Por que Engenharia Social?

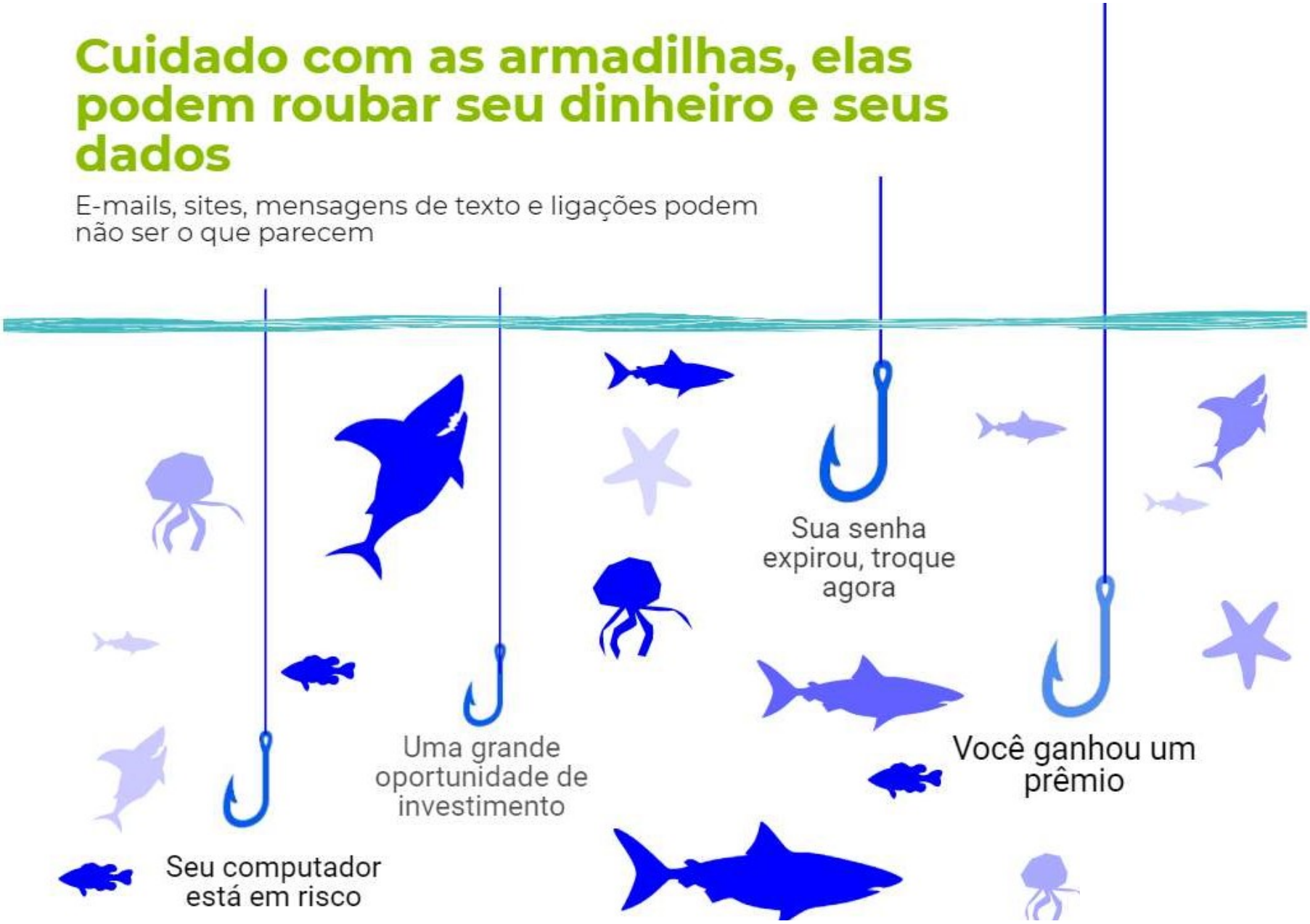
Hackear(enganar)um humano é muito mais fácil do que hackear um servidor



Táticas de Engenharia Social

Cuidado com as armadilhas, elas podem roubar seu dinheiro e seus dados

E-mails, sites, mensagens de texto e ligações podem não ser o que parecem



Brasil é o país com mais usuários atacados por phishing

Relatório aponta que um em cada cinco brasileiros recebe mensagens fraudulentas.

https://www.tecmundo.com.br/seguranca/212001-cada-cinco-brasileiros-alvo-phishing-em-2020.htm

Como detectar um ataque?

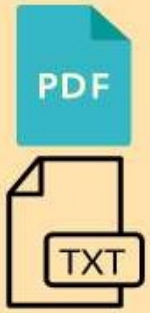
Endereço de e-mail (remetente) desconhecido.

Avisos do servidor de e-mail acusando um potencial spam.

Quais comportamentos devem ser adotados?

Extensões

Definição: as extensões de arquivos são sufixos que designam seu formato e principalmente a função que desempenham no computador.



Isso dá ao atacante inúmeras possibilidades, desde realizar a instalação de um programa no seu computador até mesmo executar um vírus dentro dele. Ou seja, tenha muita atenção antes de clicar em qualquer arquivo com o formato "exe".

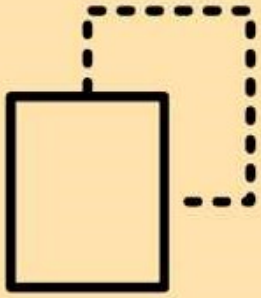
Quais comportamentos devem ser adotados?

Bloqueio de tela/conta

Inserir uma senha para bloqueio de tela/conta é uma opção muito eficiente quando se quer bloquear suas informações do acesso de terceiros. Isso evita que pessoas mexam em seu computador/celular e vejam ou tenham acesso a informações pessoais/sigilosas.

Quais comportamentos devem ser adotados?

Verificação em duas etapas



Sempre que possível ative a autenticação em duas etapas. Ex.: utilize o Google Authenticator.

Quais comportamentos devem ser adotados?

Configuração de privacidade

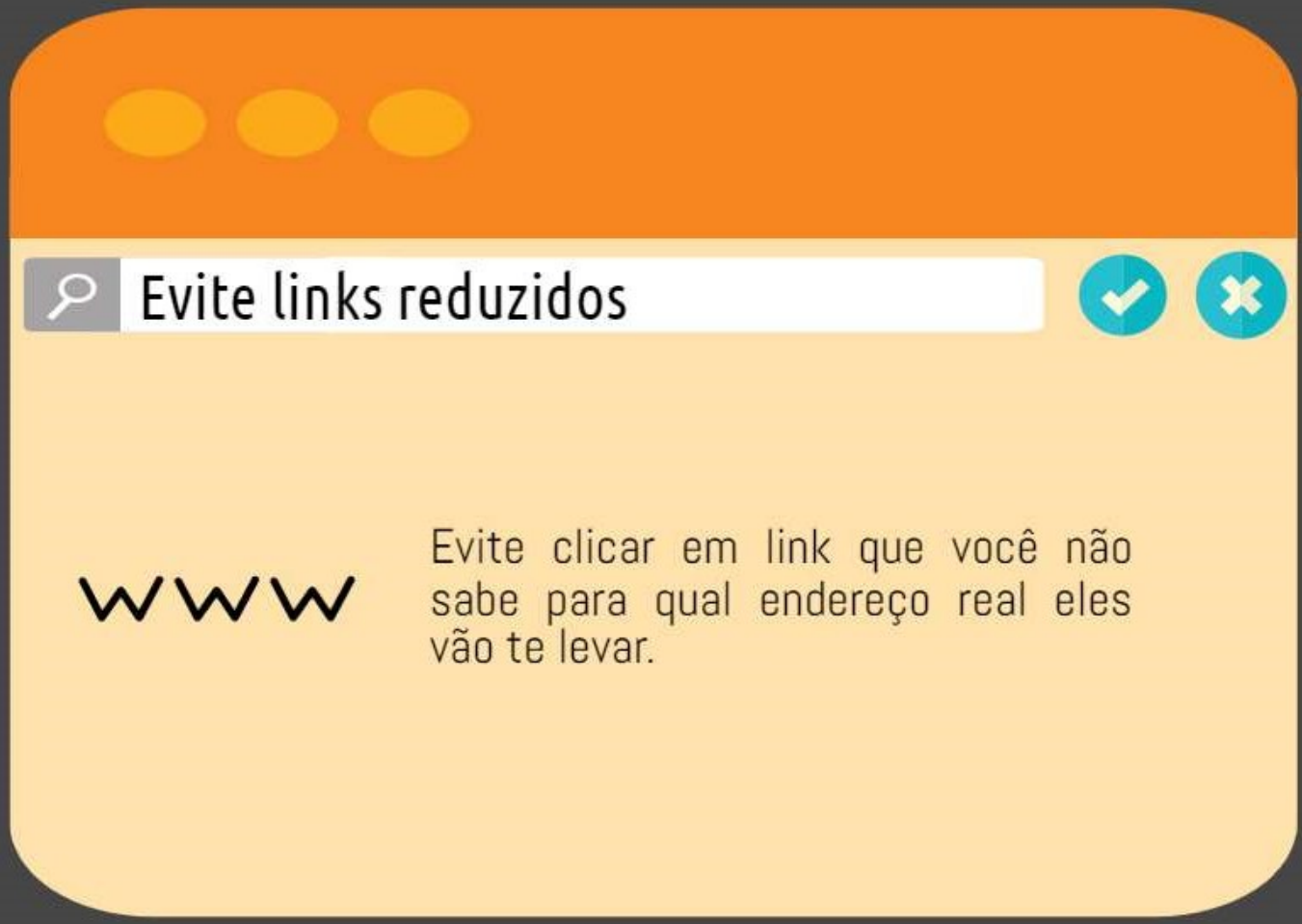
Mantenha o mínimo possível aberta suas configurações de privacidade para desconhecidos em redes sociais.

Quais comportamentos devem ser adotados?

Confirmar a fonte

Verifique por meio do google a fonte de notícias, empresas e sites que você não conhece antes de acreditar em alguma informação.

Quais comportamentos devem ser adotados?



Gato hacker invade redes de Wi-Fi mal protegidas

Bichano andava pela cidade abrindo o acesso de redes para quem estivesse por perto

Outros golpes

- Golpes do falso intermediador de vendas
- Golpe da oferta de emprego no linkedin mediante pagamento de curso
- Golpe da retirada do cartão – Com o motoboy indo a casa das pessoas


Obrigado!
Vinícius Perallis
CEO na Perallis Security
Perallis
HACK3R_
RANGERS